UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,812	12/27/2001	Eric J. Sprunk		7975

20350 7590 08/26/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

4

Office Action Summary	**Application No.** 10/049,812	**Applicant(s)** SPRUNK ET AL.	
	Examiner Brandon S. Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☒ Claim(s) *1-7* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *7-5-05*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

10

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because it contains reference numbers. International applications are allowed to contain reference numbers, however, US applications should not contain them. Correction is required. See MPEP § 608.01(b).

2. Claims 1-7 are objected to because of the following informalities:

- Claim one recites, "processing processing" in limitation one.
- Claims 2-7 depend upon claim 1 and therefore inherit its deficiencies.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent No. 5,761,306) in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 183-184 (hereinafter Schneier).

Regarding claim 1, Lewis teaches an asymmetric cryptographic processing system using a multiple key hierarchy, the asymmetric cryptographic processing system comprising

- A first key for performing asymmetric operations at a first rate, wherein each operation requires a first cryptographic processing time (fig. 2, ref. num S1 and col. 5, lines 50-55); and
- A second key for performing an asymmetric cryptographic processing operation to update the first key (fig. 2, ref. num S2 and col. 5, lines 50-55), wherein the second key requires a second cryptographic processing time greater than the first cryptographic processing time (col. 7, lines 43-50).

Lewis does not specifically teach wherein the second key is at a second rate that is less often than the first rate.

Schneier teaches wherein the second key is used in cryptographic processing operations at a second rate that is less often than the first rate (section 8.10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the second key processes at a second rate that is less than the first rate, as taught by Schneier, with the method/medium of Lewis. It would have been obvious for such modifications because different keys are used differently for different applications. Telephone communication keys should be changed with every call, whereas keys for storage of files should rarely be changed (see section 8.10 of Schneier). If the second key requires more processing time, as claimed above, it would be beneficial to change the rate of the key less than that of the first key.

Regarding claims 2-5, Lewis as modified by Schneier teaches wherein the system is used to cryptographically process and transfer digital [voice/audio/video] data in a network (see col. 1, lines 41-60 of Lewis).

Regarding claim 6, Lewis as modified by Schneier teaches wherein the second key is hard coded into the system at the time of manufacturing the system (see section 8.10 of Schneier and col. 7, lines 43-50 of Lewis, it would provide more security if the second key were hard coded into the system in a case where the second key was used for a more intensive cryptographic process and changed less often).

Regarding claim 7, Lewis as modified by Schneier teaches wherein a plurality of digital cryptographic processing systems are coupled by a telecommunications system, wherein the second key is distributed to two or more of the asymmetric cryptographic processing systems via the telecommunications system (fig. 1, ref. num 10/12/16/26 of Lewis).

Regarding claims 8 and 9, Lewis teaches a method/machine readable medium for updating keys in a digital system used to transfer data in a telecommunications system (abstract), wherein a plurality of devices are used to asymmetrically cryptographically process data (fig. 1, ref. num 12), wherein each device uses a first type of key to process the data, a second type of key to process substitute first keys, wherein the devices process data at a first rate of processing occurrences (fig. 2, ref. num S1/S2), wherein each processing occurrence requires a first amount of time (col. 5, lines 50-55), the method comprising

- Transferring cryptographically processed substitute first keys to the devices (fig. 2, ref. num S8), wherein the processing of the substitute first keys requires a second amount of time that is greater than the first amount of time (col. 7, lines 43-50).

Lewis does not teach wherein the transfers of the cryptographically processed substitute first keys occur at a second rate that is less than the first rate of processing occurrences.

Schneier teaches wherein the transfers of the cryptographically processed substitute first keys occur at a second rate that is less than the first rate of processing occurrences (section 8.10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine transferring replacement keys to the devices at a second rate that is less than the first rate, as taught by Schneier, with the method/medium of Lewis. It would have been obvious for such modifications because different keys are used differently for different applications. Telephone communication keys should be changed with every call, whereas keys for storage of files should rarely be changed (see section 8.10 of Schneier). If the second key requires more processing time, as claimed above, it would be beneficial to change the rate of the key less than that of the first key.

Regarding claim 10, Lewis teaches a method for providing secure data transactions in a telecommunications system, wherein a digital processing device receives information from the telecommunications system (abstract), wherein the digital processing device uses a first asymmetrical cryptographically processed key to perform an asymmetric cryptographic processing operation to decode the information wherein the cryptographic processing operation is at a first level of complexity requiring a first amount of resources by the processing device (fig. 2, ref. num S1/S2), wherein the cryptographic processing operation is performed at a first rate of cryptographic processing operations per unit time (col. 5, lines 50-55), the method comprising

- Transferring a second asymmetrical cryptographically processed key to the digital processing device (fig. 2, ref. num S8), wherein the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources (col. 7, lines 43-50);

- Updating the first asymmetrical cryptographically processed key from time-to-time (fig. 2, ref. num S8-S10), wherein the updating includes the following substeps;
- Encoding a substitute first asymmetrical cryptographically processed key with a second key (col. 8, lines 15-27), so that the resulting cryptographically processed substitute first asymmetrical cryptographically processed key is decodable by the second asymmetrical cryptographically processed key (col. 10, lines 17-24); and
- Transferring the substitute first asymmetrical cryptographically processed key to the digital processing device so that the substitute first asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device (col. 10, lines 30-49).

Lewis does not teach wherein the updating of the first asymmetrical cryptographically processed key occurs at a second rate of cryptographic processing operations per unit time that is less than the first rate of cryptographic processing operations per unit time.

Schneier teaches wherein the updating of the first asymmetrical cryptographically processed key occurs at a second rate of cryptographic processing operations per unit time that is less than the first rate of cryptographic processing operations per unit time (section 8.10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine transferring replacement keys to the devices at a second rate that is less than the first rate, as taught by Schneier, with the method/medium of Lewis. It would have been obvious for such modifications because different keys are used differently for different applications. Telephone communication keys should be changed with every call, whereas keys for storage of files should rarely be changed (see section 8.10 of Schneier). If the second key requires more processing time, as claimed above, it would be beneficial to change the rate of the key less than that of the first key.

Regarding claim 11, Lewis as modified by Schneier teaches further comprising

- Transferring a third asymmetrical cryptographically processed key to the digital processing device (see fig. 2, ref. num S10 of Lewis), wherein the third asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a third level of complexity requiring a third amount of resources by the processing device that is higher than the second amount of resources (see col. 7, lines 43-50 of Lewis);
- Updating the second asymmetrical cryptographically processed key from time-to-time (see fig. 2, ref. num S8-S10 of Lewis), wherein the updating of the second asymmetrical cryptographically processed key occurs at a third rate of cryptographic processing operations per unit time that is less than the second

rate of cryptographic processing operations per unit time (see section 8.10 of Schneier), wherein the updating includes the following substeps;

- Encoding a substitute second asymmetrical cryptographically processed key with a third asymmetrical cryptographically processed key (see col. 8, lines 15-27 of Lewis), so that the resulting cryptographically processed substitute second asymmetrical cryptographically processed key is capable of being cryptographically processed by the third asymmetrical cryptographically processed key (see col. 10, lines 17-24 of Lewis); and
- Transferring the substitute second asymmetrical cryptographically processed key to the digital processing device so that the substitute second asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device (see col. 10, lines 30-49 of Lewis).

Regarding claims 12-15, Lewis as modified by Schneier teaches wherein the resources include [processing time/transistor density on an IC/memory capacity/data bandwidth] (see section 8.10, page 184 of Schneier and col. 7, lines 43-48 of Lewis).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hoff
BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100